Express5800/FW300a に添付される Check Point CD-ROM が『 NG FeaturePack 3 』から『 NG with Application Intelligence (R55) 』に変更されることに伴い、ユーザーズガイドの差し替えを行います。
以下に記述する FireWall-1のコンフィグレーション、インストール箇所に関しては、本ドキュメントの記述を参照し、実施してください。

３．システムのセットアップ
　セットアップ
　　２．　システムのセットアップ
　　　　FireWall-1のコンフィグレーション　(※1)

　　３．　セキュリティポリシーのセットアップ (※2)
　　　　GUIクライアントのインストール (※3)

　再セットアップ
　　システムの再起動
　　　　再インストールの準備(SSH接続) (※4)
　　　　再インストールの手順　(※5)

４．　二重化構成について
　セットアップ
　　FireWall-1管理サーバのセットアップ (※6)
　　　　FireWall-1管理モジュールのコンフィグレーション　(※7)

　　Firewall本体のセットアップ
　　　　FireWall-1のコンフィグレーション　(※8)

　　セキュリティポリシーの設定
　　　　Firewallオブジェクトの作成　(※9)

FireWall-1 のコンフィグレーション（※1）

次に管理コンピュータからFireWall-1 付属のcpconfigコマンドを実行します。
以下の手順でコンフィグレーションを行ってください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...   ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y   ②

Please select one of the following options:
Check Point Enterprise/Pro - for headquarters and branch offices.
Check Point Express - for medium-sized businesses.
-------------------------------------------------------------------

(1) Check Point Enterprise/Pro.
(2) Check Point Express.

Enter your selection  (1-2/a-abort) [1]: 1   ③

Select installation type:
-------------------------

(1) Stand Alone - VPN-1 Pro Gateway and SmartCenter Enterprise.
(2) Distributed - VPN-1 Pro Gateway, SmartCenter and/or Log Server.

Enter your selection  (1-2/a-abort) [1]: 1   ④

IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default Filter will be applied during boot.
This program will guide you through several steps where you
will define your VPN-1 & FireWall-1 configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
```

① <Enter>キーを押すと使用許諾書が表示されますのでお読みください。

② 使用許諾に承認した場合は<Y>キーを押す。

③ インストールする製品を選択する。
ライセンスに合わせて製品を選択し、インストールします。

④ インストールするモジュールを選択する。
通常は 1 を選択し、一体型構成でインストールします。
FireWall-1管理モジュールを別マシンにインストールして管理する、分散型構成でインストールする場合は 2 を選択してください。二重化のために分散型構成でインストールする場合、以降の設定内容については「二重化構成について」を参照してください。

```
Configuring Licenses...
=======================
Host           Expiration Features

Note: The recommended way of managing licenses is using SmartUpdate.
cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [n] ? y                           ①

Do you want to add licenses [M]anually or [F]etch from file: m      ②
IP Address: 202.247.5.126
Expiration Date:
Signature Key:                                                      ③
SKU/Features:

License was added successfully

 could not put license in running module: Invalid argument


Configuring Administrators...
=============================
No VPN-1 & FireWall-1 Administrators are currently
defined for this SmartCenter Server.

Do you want to add administrators (y/n) [y] ? y                     ④
Administrator name: fws-admin
Password:                                                           ⑤
Verify Password:
Permissions for all products (Read/[W]rite All, [R]ead Only All,
[C]ustomized) w
       Permission to Manage Administrators ([Y]es, [N]o) y

Administrator fws-admin was added successfully and has
Read/Write Permission for all products with Permission to Manage
Administrators

Add another one (y/n) [n] ? n                                       ⑥
```

① <Y>キーを入力して、ライセンスを追加する。
② <M>キーを入力して、ライセンスを画面から(マニュアルで)入力する。
③ 事前に取得したライセンス情報を入力する。
ライセンスは、Firewallのライセンス製品に添付されている「ライセンス申請書」を**NSSol**へFAX して取得してください。本製品には「ライセンス申請書」は含まれていません(「Firewallの製品体系」を参照してください)。
④ <Y>キーを入力して、管理者登録を行う。
⑤ Firewall (FireWall-1) の管理者名、およびパスワード、属性を設定する。
⑥ 管理者を追加する場合は<Y>キーを、登録を終了する場合は<N>キーを押す。

```
Configuring GUI Clients...
==========================
GUI Clients are trusted hosts from which
Administrators are allowed to log on to this SmartCenter Server
using Windows/X-Motif GUI.

No GUI Clients defined
Do you want to add a GUI Client (y/n) [y] ? y ........................ ①

You can add GUI Clients using any of the following formats:
1. IP address.
2. Machine name.
3. "Any" - Any IP without restriction.
4. A range of addresses, for example 1.2.3.4-1.2.3.40
5. Wild cards - for example 1.2.3.* or *.checkpoint.com

Please enter the list of hosts that will be GUI Clients.
Enter GUI Client one per line, terminating with CTRL-D or your EOF
character.
192.168.1.99 ........................................................ ②
Is this correct (y/n) [y] ? y ....................................... ③


Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [....................] .......................................... ④

Thank you.
```

① <Y>キーを入力して、クライアントマシンのリストを新規作成する。

② セキュリティポリシーの設定を行うクライアントマシンのIPアドレスを設定する。
複数のIPアドレスを設定する場合は改行して複数行入力する。入力を終了する場合は<Ctrl>-<D>キーを押してください。

③ 入力したアドレスが正しければ<Y>キーを押す。

④ バーがフルになるまでランダムキー入力をする。

```
Configuring Certificate Authority...
====================================

The Internal CA will now be initialized
with the following name: fws.nec.co.jp

Initializing the Internal CA...(may take several minutes)
 Internal Certificate Authority created successfully
 Certificate was created successfully
Certificate Authority initialization ended successfully

Check Point product Trial Period will expire in 15 days.
Until then, you will be able to use the complete Check Point Product
Suite.
Trying to contact Certificate Authority. It might take a while...
fws.nec.co.jp was successfully set to the Internal CA

Done


Configuring Certificate's Fingerprint...
========================================
The following text is the fingerprint of this SmartCenter Server:
ADD OX GAWK MUM LONG RISK CARD FERN LILY KEY JOKE FLOC

Do you want to save it to a file? (y/n) [n] ? n ······························ ①
generating INSPECT code for GUI Clients
initial_management:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y ······································ ②
```

① GUIクライアントを接続したとき、接続したFireWall-1が正しいものであるかを確認するための文字列が表示される。
この文字列をディスク上に保存する場合は<Y>キーを、保存しない場合は<N>を入力します。

② 終了後、再起動する。
再起動後は、FireWall-1のデフォルトフィルタが有効になるため、SSH、WbMCでの接続が不可となります。

3.セキュリティポリシーのセットアップ

(※2)

セキュリティ機能をセットアップする「SmartDashboard」を管理クライアントにインストールし、編集したポリシーをインストールします。
次の条件を満たすコンピュータにSmartDashboardやその他のツールをインストールして､クライアントマシンとして使用します。

- オペレーティングシステム: Windows XP Home/professional
  Windows 98SE/Me
  Windows NT 4.0 Workstation(SP6a)
  Windows NT 4.0 Server(SP6a)
  Windows 2000 Professional(SP1、SP2、SP3、SP4)
  Windows 2000 Server(SP1、SP2、SP3、SP4)
  Windows 2000 Advanced Server(SP1、SP2、SP3、SP4)
  Windows 2003 Server
- ディスクの空き容量: 100MB以上
- メモリ: 128MB以上

※上記は、2004年3月現在の情報です。今後のパッチリリースにより変更になる可能性があります。

GUIクライアントのインストール (※3)

管理クライアントにSmartDashboardをインストールします。ここでは､SmartDashboardといっしょにログを解析するためのツール「SmartView Tracker」とシステムの状態をチェックする「SmartView Status」もインストールします。

1. コンピュータのCD-ROMドライブにCheck Point Next GenerationのCD-ROMをセットする。
   自動的にインストールプログラムが起動し、画面が表示されます。
   インストールプログラムが起動しない場合は\ wrapper \ windowsフォルダにある「demo32.exe」を実行してください。
   Welcome画面が表示されます。

2. [Next] をクリックする。
   使用許諾契約書が表示されます。

3. 内容をよく読み、同意する場合は [Yes] をクリックする。
   同意しない場合は [No] をクリックして終了します。
   [Installation Options] 画面が表示されます

4. 製品の選択を行う。
ライセンスに合わせて、[Check Point Enterprise/Pro]、[Check Point Express]を選択し、[Next]をクリックする。［Installation Options］画面が表示されます



5. ［New Installation］を選択し、［Next］をクリックする。
Product選択画面が表示されます。



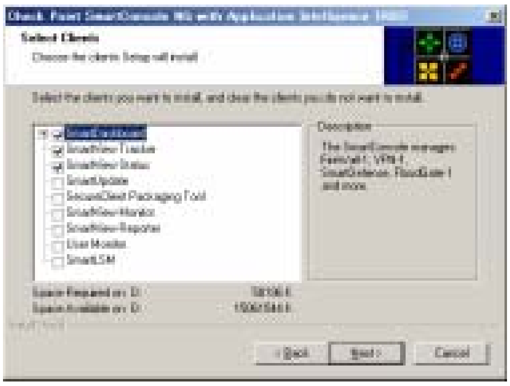
6. Management Consoleの[SmartConsole]のみにチェックし、[Next]をクリックする。



7. インストールするProductsが表示されますので、[SmartConsole]と表示されていることを確認し、[Next]をクリックする。
Choose Destination Location画面が表示されます。

8. 必要に応じてフォルダを変更し、[Next]をクリックする。
インストールするコンポーネントを選択する画面が表示されます。

9. [SmartDashboard]、[SmartView Tracker]および[SmartView Status]をチェックし、[Next]をクリックする。
インストールが開始されます。

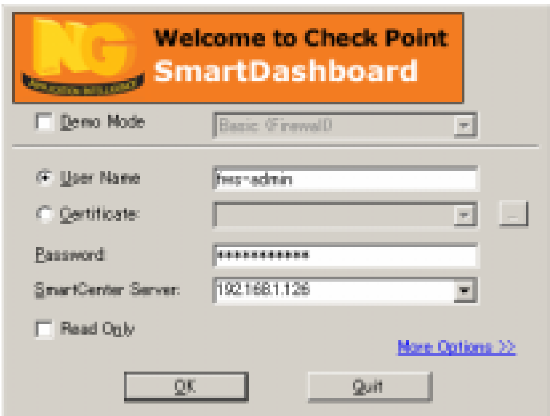


10. ショートカット作成を行うかのメッセージが表示される。
作成する場合は「はい」をクリックします。

11. Setup完了のメッセージが表示されるので、［OK］をクリックする。

12. Informationダイアログが表示されるので、［OK］をクリックする。

13. SmartDashboardを起動し、cpconfig で登録したユーザ名とパスワード、およびFirewallの内側(管理クライアント側)のアドレスを入力する。
SmartDashboardを使用し、Firewallと接続してポリシーを作成します。ネットワーク構成に応じたポリシールールを作成してください。
SmartDashboardの使い方、セキュリティポリシーの設定等についてはFireWall-1に付属のマニュアルを参照してください。

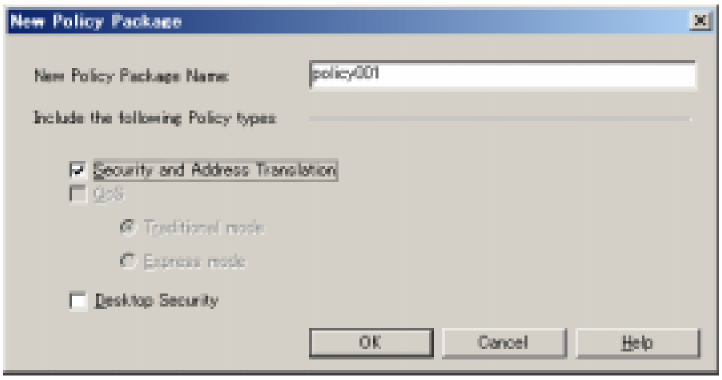


ポリシーを作成する時は、以下の手順を用いてTraditional Modeで作成することを推奨します。

14. Traditional mode の設定
SmartDashboardを起動し、接続されたらメニューバーから[Policy] - [Global Properties] のVPNページにおいて、「Traditional mode to all new Security Policies: Setup with Encryption Rules.」を選択し、[OK]をクリックする。



15. メニューバーから [File]-[New]を選択し、Policy Package Nameを設定する。
新しいポリシー画面が作成され、ポリシーの設定が可能となります。



【重要】
Firewall と管理クライアントとの設定において、SSH を使用しますので、FireWall-1 のポリシーに、管理クライアントから Firewall に対して SSH のポート番号へのアクセスを許可するためのルールを追加してください。このとき、接続元には必ず管理クライアントのみを設定し、他のホストからのアクセスは許可しないようにしてください。

再インストールの準備(SSH準備)（※4)

作業を行うためには、SSH接続用管理クライアントが必要です。本体の電源がOFFの状態で、SSH接続用管理クライアントを本体背面のLANポートインタフェース(内部ネットワーク用)にクロスケーブル接続してください。また、Firewallに直接LANケーブルを接続しないで、内部ネットワークに接続する場合は、ハブなどにLANケーブルで接続してください。

Firewallとの接続に必要なもの

- SSH接続用管理クライアント
- LANケーブル

再インストールに必要なディスク

あらかじめ以下のディスクを用意してください。

- バックアップCD-ROM
- Check Point Next Generation(NG with Application Intelligence R55)
- 再インストール用ディスク
- 初期化導入設定用ディスク
- バックアップディスク(任意)

再インストール手順（※5）

1. 本体の電源をONにし、前面にあるフロッピーディスクドライブに再インストール用ディスクを、CD-ROMドライブにバックアップCD-ROMをセットする。

   自動的にプログラムCD-ROMからのインストールが始まります。

   インストールは約10分で完了します。
   インストールを完了すると、CD-ROMドライブからバックアップCD-ROMが排出されます。
   本体は、電源が入った状態で、システムが停止している状態になります。

2. バックアップCD-ROMおよび再インストール用ディスクを取り出した後、POWERスイッチを押して電源をOFFにする。

3. 初期導入設定用ディスクをセットし、POWERスイッチを押して電源をONにする。
   初期導入設定用ディスクは、初期導入設定用ツールで作成済みのものとします。
   しばらく（3分程度）してから管理クライアントからSSHクライアントにて、Firewallへログインします。

4. 管理クライアントから初期導入設定用ツールで設定したSSHの「管理者アカウント名」と「Password」を利用し、ログインする。

5. <バックアップしておいた設定をリストアする場合>
   以下のコマンドを実行して設定を行う。
   設定をバックアップしたフロッピーディスクを本体にセットしてください。

```
# fwrestore -i
Please insert backup floppy disk. (#1)
Press enter key.
restore fws.ini ...
restore clp.conf ...
restore .http...
restore .ssh...
restore completed.
After turned off FDD access light, Press enter key.
# fwsetup -i /opt/necfws/etc/fws.ini
       :
       :
# shutdown -r now
```

バックアップディスクをセットして、<Enter>キーを押す（Press enter key.）

二重化構成を使用していない場合は表示されない（restore clp.conf ...）

フロッピーディスクドライブのアクセスランプが消えたら<Enter>キーを押し、その後フロッピーディスクを取り出す（After turned off FDD access light, Press enter key.）

終了後、再起動する（# shutdown -r now）

<バックアップのリストアをしない場合>
本章の「2．システムのセットアップ」-「基本設定ツールによる設定」を参照して設定を行い、終了後、再起動する。

6. 起動後、CD-ROMドライブにCheck Point Next Generation（NG with Application Intelligence　R55）のCD-ROMをセットし、FireWall-1のモジュールを以下の手順で適用する。

```
# mount /dev/cdrom
# cd /mnt/cdrom/linux/
# rpm -i ./CPshared-50/CPshrd-R55-00.i386.rpm
# rpm -i ./CPFirewall1-50/CPfw1-R55-00.i386.rpm
# cd /
# umount /dev/cdrom
```

7. CD-ROMドライブからCD-ROMを取り出し、再起動する。

```
# shutdown -r now
```

8. cpconfigを実行してFireWall-1の設定を行う。
cpconfigについては本章の「2. システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

```
# cpconfig
   :
   :
Do you want to reboot? (y/n) [y] ? y
```

9. ポリシーの作成を行う。
<あらかじめバックアップしておいた設定をリストアする場合>
以下のコマンドを実行してFireWall-1の設定をする。

```
# cpstop
# fwrestore -f
Please insert backup floppy disk. (#1)
Press enter key.
There is 1 floppy disk for restore.
restore fw config files...(1/1)
restore completed.
After turned off FDD access light, Press enter key.
# cpstart
```

- # cpstop：FireWall-1を停止する
- # fwrestore -f：バックアップディスクをセットして、<Enter>キーを押す
- After turned off FDD access light, Press enter key.：フロッピーディスクドライブのアクセスランプが消えたら<Enter>キーを押し、その後フロッピーディスクを取り出す
- # cpstart：FireWall-1を起動する

<バックアップのリストアをしない場合>
SmartDashboardを使用してポリシーを作成する。

10. SmartDashboardでポリシーをインストールする。

【 重要 】
CD-ROMドライブにCheck Point Next Generation（NG with Application Intelligence R55）のCD-ROMをセットした状態のままFirewall本体を起動しないように注意してください。

FireWall-1 管理サーバのセットアップ

(※6)

二重化する 2 台のサーバを管理するための管理サーバをセットアップします。以下の条件を満たすコンピュータに管理モジュールをインストールしてください。Express5800/FW300 または FW500 をもう 1 台用意し、管理サーバとして動作させることも可能です。

オペレーティングシステム: Windows NT 4.0 Server(SP6a)、
Windows 2000 Server(SP1、SP2、SP3、SP4)、
Windows 2000 Advanced Server(SP1、SP2、SP3、SP4)、
Windows 2003 Server、
Solaris8 / UltraSPARC (32-bit、64-bit)、
Solaris9 / UltraSPARC (64-bit)、
RedHat Linux 7.0 (kernel version 2.2.16、2.2.17、2.2.19)
RedHat Linux 7.2 (kernel version 2.4.9-31)
RedHat Linux 7.3 (kernel version 2.4.18-5、2.4.18-27、
2.4.20)

Windows or Linux
ディスク容量: 300MB以上
メモリ: 128MB以上

Solaris
ディスク容量: 300MB以上
メモリ: 128MB以上

※上記は、2004年3月現在の情報です。今後のパッチリリースにより変更になる可能性があります。

FireWall-1管理モジュールのコンフィグレーション（※7）

管理モジュールを管理サーバへインストールします。以下の手順でコンフィグレーションを行ってください。図中の〈略〉の設定する項目については、3章の「2. システムのセットアップ」-「FirewWall-1のコンフィグレーション」を参照してください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...  ······························· ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y ········ ②

Please select one of the following options:
Check Point Enterprise/Pro - for headquarters and branch offices.
Check Point Express - for medium-sized businesses.
-------------------------------------------------------------------

(1) Check Point Enterprise/Pro.
(2) Check Point Express.

Enter your selection  (1-2/a-abort) [1]: 1 ···························· ③

Select installation type:
-------------------------

(1) Stand Alone - install VPN-1 Pro Gateway and SmartCenter Enterprise.
(2) Distributed - install VPN-1 Pro Gateway, SmartCenter and/or Log Server.

Enter your selection  (1-2/a-abort) [1]: 2 ···························· ④
```

① FireWall-1管理モジュールのコンフィグレーションをする。
② 使用許諾に承認した場合は<Y>キーを押す。
③ インストールする製品を選択する。
　ライセンスに合わせて製品を選択し、インストールします。
④ インストールするモジュールを選択する。
　二重化構成の場合は「2」を選択し、インストールします。

```
Select installation type:
-------------------------

(1) VPN-1 Pro Gateway.
(2) Enterprise SmartCenter.
(3) Enterprise SmartCenter and VPN-1 Pro Gateway.
(4) Enterprise Log Server.
(5) VPN-1 Pro Gateway and Enterprise Log Server.

Enter your selection  (1-5/a-abort) [1]: 2 ······························· ①


Please specify the SmartCenter type you are about to install:
-------------------------------------------------------------

(1) Enterprise/Pro Primary SmartCenter.
(2) Enterprise/Pro Secondary SmartCenter.

Enter your selection  (1-2/a-abort) [1]: 1 ······························· ②
This program will guide you through several steps where you
will define your SVN Foundation configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
           :
          (略)
           :
************* Installation completed successfully *************

Do you wish to start the installed product(s) now? (y/n) [y] ? y ········· ③
cpstart: Power-Up self tests passed successfully
           :
          (略)
           :
FireWall-1: This is a Management Station. No security policy will be loaded
FireWall-1 started

# shutdown -r now ········································· ④
```

① インストールするモジュールを選択する。
「2」を選択し、管理モジュールをインストールします。

② インストールする管理モジュールのタイプを選択する。
「1」を選択し、Primaryとして使用します。

③ 管理モジュールを起動させる。

④ 再起動する。

Firewall 本体のセットアップ

FireWall-1のコンフィグレーション (※8)

二重化構成の場合、コンフィグレーション手順が3章とは一部異なります。図中の〈略〉の設定する項目については、3章の「2. システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...                                              ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y         ②

Please select one of the following options:
Check Point Enterprise/Pro - for headquarters and branch offices.
Check Point Express - for medium-sized businesses.
-------------------------------------------------------------------

(1) Check Point Enterprise/Pro.
(2) Check Point Express.

Enter your selection  (1-2/a-abort) [1]: 1                              ③

Select installation type:
-------------------------

(1) Stand Alone - install VPN-1 Pro Gateway and SmartCenter Enterprise.
(2) Distributed - install VPN-1 Pro Gateway, SmartCenter and/or Log Server.

Enter your selection  (1-2/a-abort) [1]: 2                              ④
```

① FireWall-1管理モジュールのコンフィグレーションをする。
② 使用許諾に承認した場合は<Y>キーを押す。
③ インストールする製品を選択する。
　ライセンスに合わせて製品を選択し、インストールします。
④ インストールするモジュールを選択する。
　二重化構成の場合は「2」を選択し、インストールします。

```
Select installation type:
-------------------------

(1) VPN-1 Pro Gateway.
(2) Enterprise SmartCenter.
(3) Enterprise SmartCenter and VPN-1 Pro Gateway.
(4) Enterprise Log Server.
(5) VPN-1 Pro Gateway and Enterprise Log Server.

Enter your selection  (1-5/a-abort) [1]: 1 ........................................ ①


Is this a Dynamically Assigned IP Address Module installation ? (y/n) [n] ? ...... ②
Would you like to install a Check Point clustering product (CPHA, CPLS or State
Synchronization)? (y/n) [n] ? y ................................................... ③

IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default Filter will be applied during boot.
This program will guide you through several steps where you
will define your VPN-1 & FireWall-1 configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
                              :
                             (略)
                              :
```

① インストールするモジュールを選択する。
「1」を選択し、インストールします。

② Dynamically Assigned IP Address Moduleをインストールするか問い合わせがあるので、<Enter>キーを選択する。

③ Check Point clustering productをインストールするか問い合わせがあるので、<Y>キーを押す。

```
                              :
                             (略)
                              :
Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized ┐
Enter Activation Key:      │ ①
Again Activation Key:      ┘

The Secure Internal Communication was successfully initialized

initial_module:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y  ②
```

① FireWall-1管理サーバとFirewall間での通信に使用するパスワードを設定してください。
② 終了後、再起動します。

セキュリティポリシーの設定

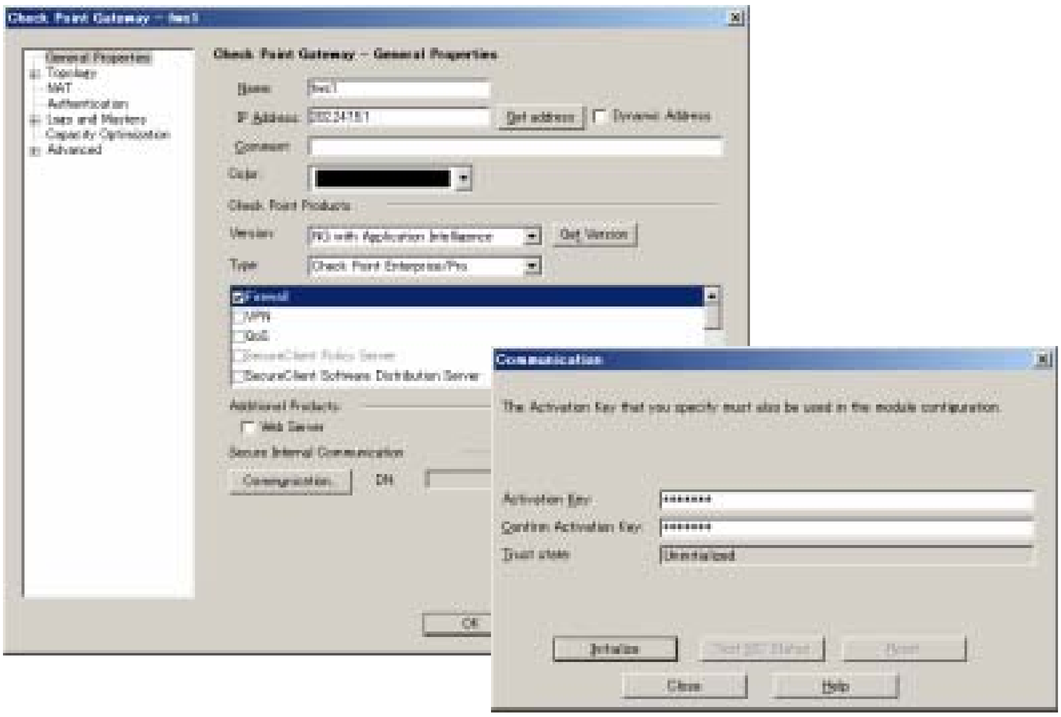
Firewallオブジェクトの作成（※9）

1.2台のFirewallのオブジェクトを作成する。

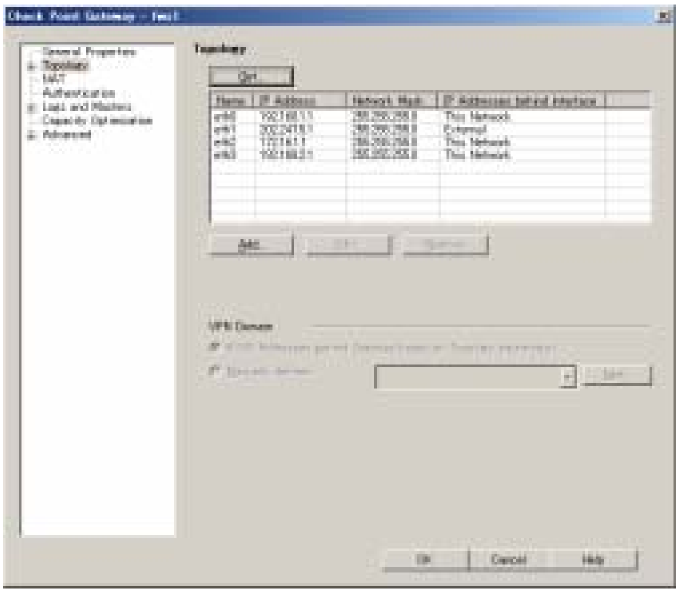
ーViewObjectTree の［CheckPoint］を選択し、右クリックします。
［New Check Point］→［Gateway］を選択します。

ーオブジェクト：Gateway
名前　　　　：fws1、fws2
内容　　　　：IP Address には FireWall-1 管理サーバと同じネットワークの実 IP アドレスを設定してください。

ーFireWall-1 管理サーバから Firewall を管理（セキュリティポリシーの設定やログ表示など）するためには、FireWall-1 管理サーバと Firewall との間で通信を行うための設定が必要です。General ページで［Communication...］をクリックし、FireWall-1 のコンフィグレーション時に設定したパスワードを入力してください。



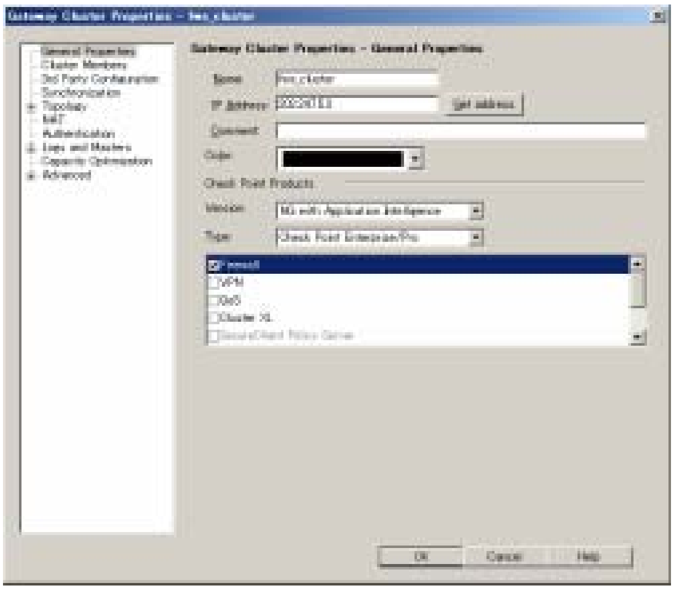
ーTopology ページで全インタフェースを設定します。[Get Topology...] をクリックして自動取得
　します。



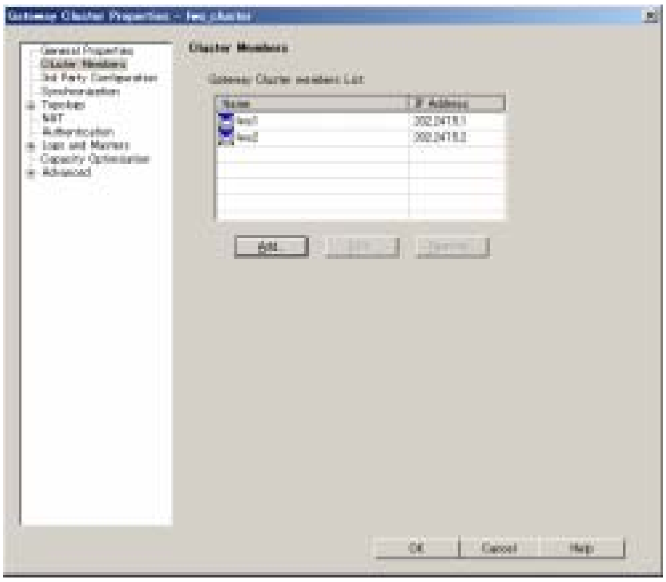
2.以下のクラスタオブジェクトを作成する。

ーViewObjectTree の［CheckPoint］を選択し、右クリックします。
　［New Check Point］→［Gateway Cluster］を選択します。

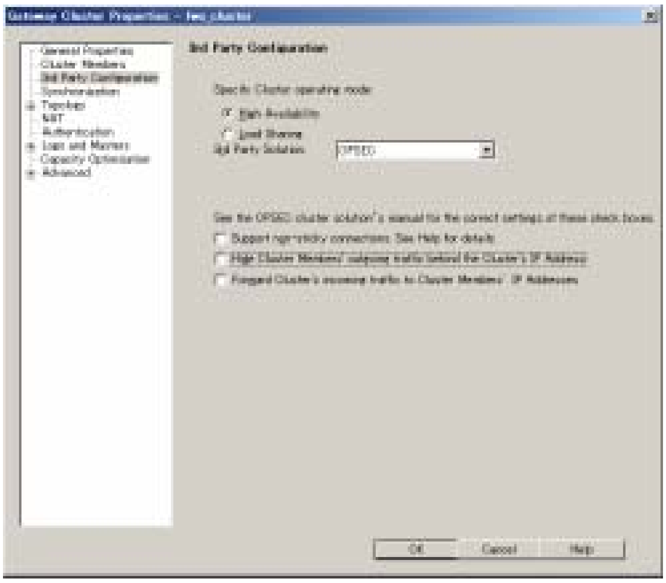
ーオブジェクト: Gateway Cluster
　名前　　　　: fws_cluster
　内容　　　　: IP Address にはインターネット側の仮想 IP アドレスを指定してください。



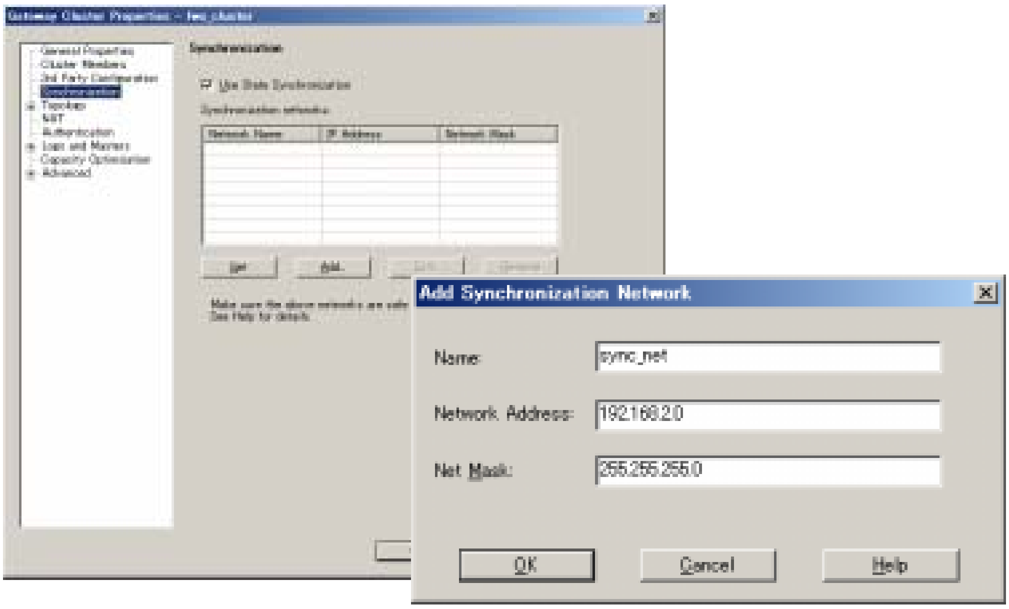
3.Cluster Membersページで、手順１で作成した２台のFirewallオブジェクト（fws1とfws2）を追加する。



4.3rd Party Configurationページで、設定を確認する。
「Hide Cluster Members’ outgoing traffic behind the Cluster’s IP Address」にチェックが付いていないことを確認します。



5.Synchronizationページでセッション同期を行うネットワークを入力する。
　このネットワークにおいて互いのコネクション情報を共有します。



6.Topologyページにてインターフェースの設定する。
　IPアドレスには、仮想IPアドレスを設定します。

